Introduction

What is a computer network?

Components of a computer network:

- host devices (PCs, servers, laptops, handhelds)
- routers & switches (IP router, Ethernet switch, WiFi routers)
- links (wired, wireless, quantum)
- protocols (IP, TCP, CSMA/CD or CA, BGP)
- applications (SMTP, DNS, HTTP, SNMP)
- humans and bots (spam, DoS, worm)

Hosts, routers & links form the *hardware* side.

Protocols & applications form the *software* side.

Protocols can be viewed as the "glue" that binds everything else together.

Protocol example: low- to high-layer

- NIC (network interface card): hardware
  → e.g., Ethernet card, WLAN card, CDMA or TDMA air interface (cell phones)
  → what about USB and FireWire?
- NIC firmware: software side of NIC
  → mainly ROM code
- device driver: part of OS
  → fast and slow interrupt handlers
- ARP, RARP: OS
  → NICs have two names (48 vs. 32 bits): translation
- IP: OS
  → defining software glue of global Internet
  → hosts, routers, cell phones

- OSPF, RIP, BGP: protocols above IP running at routers

  → OFPF, RIP: within organizations (intra-domain)

  → BGP: global Internet (inter-domain)

- TCP, UDP: OS

  → TCP: files (text, image, video)

  → UDP: multimedia streaming

  → hybrids and exceptions to the rule

  → transport protocols: host OS

- DNS, HTTP, SMTP, SNMP: application layer
- ssh, web browser, php, P2P (BitTorrent), YouTube, Facebook, Twitter: application layer
- humans, bots (web crawlers, network monitors)

What layers are important?

- 1970s: lower layers and hardware
- 1980s: both lower and higher layers
- 1990s: higher layers
- 21st century: both lower and higher layers, and hardware

  $\rightarrow$ driving force: wireless networks

  $\rightarrow$ boundary between telephony and data networks: (almost) gone

Fast moving environment

Example: Digital TV and freed-up UHF spectra

→ 300–700 MHz frequency may be used for data networking

→ e.g., super WiFi

Example: Short-distance communication services

→ RFID for inventory control, electronic payments

→ getting rid of wires: e.g., wireless USB

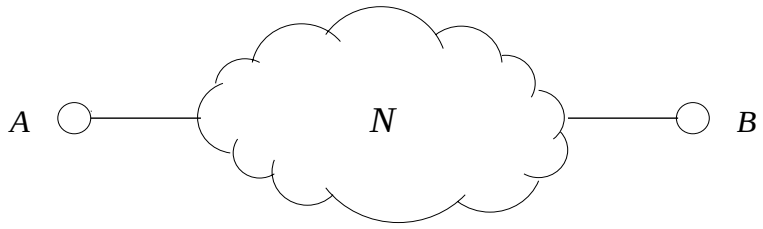
Sound technical grounding in wireless: critical for adapting to future changes

→ not just for network/IT industry

Computer Networks: enable communication

Simplest instance of communication problem:

> Two hosts A, B are connected by some network N. Transmit information between A and B.



Network N can take many forms

$\rightarrow$ single wire: point-to-point link

$\rightarrow$ global Internet

Necessary capabilities of A, B, and N

$\rightarrow$ functional requirements

1. Information abstraction

- representation as objects (e.g., text files, binary executables, audio, video, voice)

  $\rightarrow$ high-level representation

- bytes & bits

  $\rightarrow$ digital representation

  $\rightarrow$ low-level representation

- signals over physical media

  $\rightarrow$ electromagnetic waves

  $\rightarrow$ analog (sine) or digital (square)

  $\rightarrow$ dominant today: analog transmission

Minimal tasks performed by A, B

- encode information
- decode information

  $\rightarrow$ data representation & translation

  $\rightarrow$ convention A and B agree upon

  $\rightarrow$ preparation step before actual physical (wired or wireless) transmission

Example:

- little endian vs. big endian

  $\rightarrow$ mundane but necessary

- length of message

  $\rightarrow$ fixed or variable length

  $\rightarrow$ fixed: header; variable: payload

  $\rightarrow$ maximum length cap imposed ($\neq$ enforced)

Additional tasks A and B may perform (depends on network environment):

- information corruption: bits flip

  $\rightarrow$ called bit error rate (BER)

  $\rightarrow$ 10^{-9} for fiber optic cable

  $\rightarrow$ 10^{-6} or higher for wireless

- information loss: packet drop at routers and hosts

  $\rightarrow$ buffers are full

- information delay: queueing at buffers, processing delay

  $\rightarrow$ bad for voice, real-time video, games

- information security

  $\rightarrow$ protect against eavesdropping: confidentiality

  $\rightarrow$ protect against ID theft: authentication

  $\rightarrow$ protect against tampering: integrity

Network N connecting two or more hosts can be of three types:

- point-to-point link
- multi-access link
- internetwork

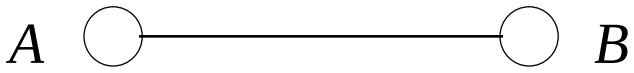
Network medium may be

- wired
- wireless

Host (e.g., node, station, device, router) may be

- stationary
- mobile

Point-to-point link



- NIC at A, NIC at B
- physical wire between the two NICs
- various wired cables

  → copper and fiber of different quality/grade
- wireless medium

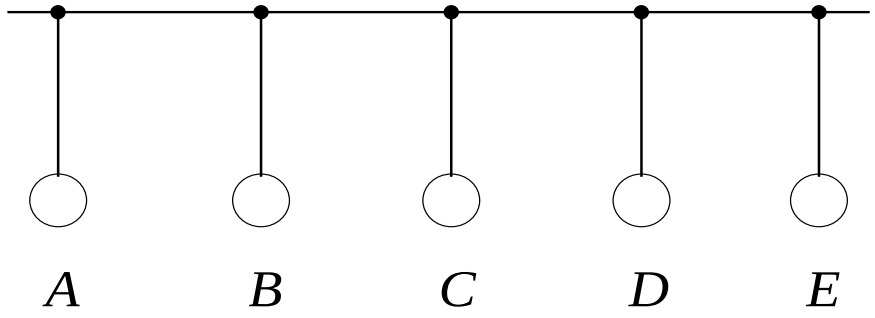
  → line of sight

  → directional antennas

  → e.g., roof-top building-to-building, infrared TV remote
- no addressing (i.e., names) necessary

  → but special case

Multi-access link



- bus (e.g., old Ethernet)
- wireless media

  → omni-directional antennas (e.g., wireless LANs)
- broadcast: everyone connected or within range can hear everything
- addressing (i.e., naming) necessary

  → "From" and "To"

  → single destination: unicasting

  → multiple destinations: multicasting

- multi-user communication or access control: who gets to use link when

  → multi-access link: shared resource

  → myriad of LAN technologies and protocols

  → computer motherboard: bus arbitration